МЕДИЦИНА, ПЕДАГОГИКА И ТЕХНОЛОГИЯ:
ТЕОРИЯ И ПРАКТИКА
Researchbib Impact factor: 11.79/2023
SJIF 2024 = 5.444
Том 2, Выпуск 4, 30 Апрел

ZAMONAVIY SHIFRLASH ALGORITMLARNING BARDOSHLILIGI

Toshboyeva Feruza To'lqin qizi
Toshkent davlat iqtisodiyot universiteti

Annotatsiya: Mazkur maqola zamonaviy ma'lumotlarni shifrlash algoritmlarini tahlil qilishga bag'ishlangan. Kirish AES va RSA kabi eng keng tarqalgan shifrlash algoritmlari haqida umumiy ma'lumot beradi. Maqolaning asosiy qismi zamonaviy shifrlash algoritmlarining zaif tomonlarini tahlil qilishni o'z ichiga oladi va turli xil hujum usullarini ko'rib chiqadi. Umumiy qilib aytganda, ma'lumotlarni himoya qilishning kompleks usullarini qo'llash va mumkin bo'lgan hujumlarning oldini olish uchun foydalaniladigan shifrlash algoritmlarini vaqti-vaqti bilan yangilab turish kerak degan xulosaga keldi.

Kalit so'zlar: shifrlash algoritmi, bloklash, ma'lumotlar xavfsizligi, zaiflik, hujum usuli, kompleks usul, ma'lumotlarni himoya qilish.

СТАБИЛЬНОСТЬ СОВРЕМЕННЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Аннотация: Данная статья посвящена анализу современных алгоритмов шифрования данных. Во введении представлен обзор наиболее распространенных алгоритмов шифрования, таких как AES и RSA. Основная часть статьи включает в себя анализ слабых сторон современных алгоритмов шифрования и рассматривает различные методы атак. В целом был сделан вывод, что используемые алгоритмы шифрования должны время от времени обновляться, чтобы применять сложные методы защиты данных и предотвращать возможные атаки.

Ключевые слова: алгоритм шифрования, блокировка, безопасность данных, уязвимость, метод атаки, комплексный метод, защита данных.

STABILITY OF MODERN ENCRYPTION ALGORITHMS

Abstract: This article is devoted to the analysis of modern data encryption algorithms. The introduction provides an overview of the most common encryption algorithms, such as AES and RSA. The main part of the article includes an analysis of the weaknesses of modern encryption algorithms and considers various attack methods. In general, it was concluded that the encryption algorithms used should be

updated from time to time in order to apply complex methods of data protection and prevent possible attacks.

Key words: encryption algorithm, blocking, data security, vulnerability, attack method, complex method, data protection.

KIRISH

Ma'lumotlarni shifrlash - bu xom ma'lumotlarni maxsus kalitsiz o'qib bo'lmaydigan shifrlangan shaklga aylantirish jarayoni. Ko'pgina shifrlash algoritmlari mavjud, ammo ularning hammasi ham nozik ma'lumotlarni himoya qilish uchun yetarli xavfsizlikni ta'minlamaydi. Eng keng tarqalgan shifrlash algoritmlari orasida AES va RSA [1,2]. AES (Advanced Encryption Standard) - bu ma'lumotlarning maxfiyligini himoya qilish uchun ishlatiladigan simmetrik blokli shifrlash algoritmi [2]. AES blokli shifrlashdan foydalanadi, ya'ni u ma'lumotlarni qattiq o'lchamdagi bloklarda (odatda 128 bit) shifrlaydi. RSA (Rivest-Shamir-Adleman) assimetrik shifrlash algoritmi bo'lib, ma'lumotlar yaxlitligi va autentifikatsiyasini himoya qilish uchun ishlatiladi. Bu algoritm ma’lumotlarni shifrlash uchun matematik transformatsiyalardan foydalanadi [2,3].

Biroq, hatto bu algoritmlar ham butunlay xavfsiz emas. Ba'zi zaifliklardan ushbu algoritmlar yordamida shifrlangan ma'lumotlarga hujum qilish uchun foydalanish mumkin [5].

Shunday qilib, AES algoritmi bilan shifrlangan ma'lumotlarning shifrini ochish uchun quyidagi turdagi hujumlardan foydalanish mumkin:

1-jadval

AES algoritmi uchun hujumlar turlari

№	Hujum nomi	Tavsif
1	2	3

	Qo'pol kuch usuli	Bu hujum usuli bo'lib, unda tajovuzkor barcha mumkin bo'lgan shifrlash kalitlarini to'g'ri hal qilish natijasini topmaguncha sinab ko'radi. Agar shifrlash kaliti yetarlicha uzun bo'lsa, bu hujum juda sekin bo'lishi mumkin, ammo kalit qisqa bo'lsa samarali bo'lishi mumkin.
2	Bajarilish vaqtini tahlil qilish usuli	shifrlash kalitini hisoblash uchun shifrlashning bajarilish vaqti haqidagi ma'lumotlardan foydalanadigan usuldir. Ushbu hujum usuli, agar tajovuzkor shifrlash sodir bo'lgan kompyuterga kirish imkoniga ega bo'lsa samarali bo'lishi mumkin.
3	Lug'at usuli	Bu hujum usuli bo'lib, tajovuzkor shifrlash kalitini qo'pol kuch bilan ishlatish uchun oldindan tayyorlangan parollar yoki kalitlarning lug'atidan foydalanadi. Agar shifrlash kaliti lug'atdagi so'z yoki ibora bo'lsa, bu hujum samarali bo'lishi mumkin.
4	Chiziqli kriptoanaliz usuli	Tajovuzkor kirish ma'lumotlari, chiqish ma'lumotlari va shifrlash kaliti o'rtasidagi bog'liqlikni topish uchun statistik tahlillardan foydalanadigan hujum usulidir. Agar tajovuzkor katta hajmdagi kirish va chiqish ma'lumotlariga kirish imkoniga ega bo'lsa, bu hujum usuli samarali bo'lishi mumkin.

5	Differensial kriptoanaliz usuli	Bu tajovuzkor bir xil shifrlash kaliti bilan shifrlangan ikkita xabardagi farqlarni qidiradigan hujum usuli. Ushbu hujum usuli, agar tajovuzkor ko'p sonli xabarlar juftligiga kirish imkoniga ega bo'lsa va kirish ma'lumotlari, chiqish ma'lumotlari va shifrlash kaliti o'rtasidagi bog'liqlikni topish uchun tahlilni amalga oshira olsa samarali bo'lishi mumkin.
6	O'lchovni kamaytirish usuli	ma'lumotlar shifrini ochish muammosining o'lchamini kamaytirish uchun matematik usullardan foydalanadigan hujum usuli bo'lib, uni hal qilishni osonlashtiradi. Agar tajovuzkor etarlicha katta miqdordagi ma'lumotlarga ega bo'lsa, bu hujum usuli samarali bo'lishi mumkin.
7	Korrelyatsiya statistikasi usuli	kirish ma'lumotlari, chiqish ma'lumotlari va shifrlash kaliti o'rtasidagi bog'liqlikni aniqlash uchun korrelyatsiya tahlillaridan foydalanadigan hujum usuli. Ushbu hujum usuli, agar tajovuzkor etarlicha katta miqdordagi kirish va chiqish ma'lumotlariga ega bo'lsa samarali bo'lishi mumkin.

Shuni ta'kidlash kerakki, ushbu hujum usullarining aksariyati murakkab va sezilarli hisoblash resurslarini talab qiladi [6,7]. Bundan tashqari, kuchli shifrlash kalitlaridan foydalanish, shuningdek, shifrlash algoritmini to'g'ri amalga oshirish tizimga muvaffaqiyatli hujum qilish ehtimolini sezilarli darajada kamaytirishi mumkin.

RSA algoritmi bilan shifrlangan ma'lumotlarning shifrini ochish uchun quyidagi turdagi hujumlardan foydalanish mumkin:

2 - jadval

RSA algoritmi uchun hujumlar turlari:

№	Hujum nomi	Tavsif
1	2	3
1	Faktorizatsiya usuli	RSA katta raqamlarni faktoring qilish qiyinligiga asoslanadi. Biroq, agar tajovuzkor xabarni shifrlash uchun ishlatiladigan N raqamini faktor bilan ta'minlay olsa, u maxfiy kalitni olishi va xabarning shifrini ochishi mumkin. Buning uchun Fermaning faktorizatsiya usuli va sonli elak usuli kabi faktorizatsiya algoritmlaridan foydalaniladi.
2	Matnni tanlash usuli	agar tajovuzkor bir xil ma'lumotni o'z ichiga olgan bir nechta shifrlangan xabarlarni olishi mumkin bo'lsa, u ulardan bir xil ochiq kalit yordamida shifrlangan boshqa xabarlarning shifrini ochish uchun foydalanishi mumkin.
3	Qayta foydalanish usuli	agar tajovuzkor shifrlangan xabarni tutib olsa, uni serverga qayta yuborishi mumkin, bu esa xabarning shifrini ochish uchun bir xil ochiq kalitdan foydalanadi. Buzg'unchi maxfiy kalitni olish uchun natijada

		shifrlangan xabardan foydalanishi mumkin.
4	Ochiq kalitni tanlash usuli	agar tajovuzkor xabar RSA yordamida shifrlanganligini bilsa, u p va q uchun hammaga ma'lum bo'lgan qiymatlardan foydalangan holda ochiq kalitni taxmin qilishga harakat qilishi mumkin. Bu hujum Bonnington hujumi deb ataladi.
5	Qo'pol kuch usuli	Agar tajovuzkor shifrlangan xabarni ushlay olsa va xabar past entropiyaga ega ekanligini bilsa (ya'ni, unda tasodifiylik kam bo'lsa), u xabarni parolini ochish uchun barcha mumkin bo'lgan kombinatsiyalarni sinab ko'rish uchun qo'pol kuch hujumidan foydalanishi mumkin.
6	Vaqt usuli	agar tajovuzkor shifrlangan xabarning shifrini ochish uchun zarur bo'lgan vaqtni o'lchashi mumkin bo'lsa, u bu ma'lumotdan maxfiy kalitni olish uchun foydalanishi mumkin. Buning uchun tajovuzkor serverga ko‘plab shifrlangan xabarlarni yuborishi, har birining shifrini ochish uchun zarur bo‘lgan vaqtni o‘lchashi va har bir xabarning shifrini ochish vaqtini solishtirishi mumkin. Agar xabarning shifrini ochish vaqti maxfiy kalitga bog'liq bo'lsa, tajovuzkor ushbu ma'lumotdan maxfiy kalitning qiymatlarini

		aniqlash uchun foydalanishi mumkin.
7	Xato usuli	Agar tajovuzkor bir nechta shifrlangan xabarlarni to'xtata olsa, u maxfiy kalitning qiymatini aniqlash uchun xato hujumidan foydalanishi mumkin. Ushbu hujum, agar kalit qiymatlari noto'g'ri bo'lsa, xabarni shifrlashda xatolik yuz berishi mumkinligiga asoslanadi. Buzg'unchi ushbu ma'lumotdan to'g'ri kalit qiymatlarini aniqlash uchun foydalanishi mumkin.
8	Soxtalashtirish usuli	Agar tajovuzkor RSA yordamida shifrlangan xabarlarga ta'sir eta olsa, u o'zining xabarlarini yaratish uchun soxtalashtirilgan hujumdan foydalanishi mumkin, ular tajovuzkor xohlagan tarzda shifrlanadi.

Umuman olganda, RSA usuli yordamida shifrlangan ma'lumotlarni himoya qilish uchun quyidagi choralarni ko'rish kerak [8]:

1. Faktorizatsiya hujumlarining oldini olish uchun p va q tub sonlaridan foydalanib kalitlarni yarating.

2. Qo'pol kuch hujumlaridan himoya qilish uchun etarlicha uzun kalitlardan foydalaning.

3. Ruxsatsiz kirishning oldini olish uchun shaxsiy kalitni xavfsiz joyda saqlang.

4. Shifrlangan ma'lumotni tajovuzkorlar tomonidan ushlab qolish va parolini ochishdan himoya qilish uchun uni uzatishda xavfsiz ma'lumotlarni uzatish protokolidan foydalaning.

5. Tizimda yuzaga kelishi mumkin bo'lgan zaifliklarni oldini olish uchun kalitlarni muntazam yangilab turing.

6. Xabarlarning haqiqiyligini tasdiqlash uchun raqamli imzo qo'shish yoki shaxsiy kalitga ruxsatsiz kirishdan himoya qilish uchun ikki faktorli autentifikatsiyadan foydalanish kabi qo'shimcha xavfsizlik choralarini qo'llang.

Ma'lumotlar xavfsizligini yaxshilashga yordam beradigan foydalanuvchi tavsiyalari:

1. Axborot xavfsizligi darajasini oshirish uchun kompleks himoya usullaridan foydalanish zarur [9-11]. Bunday usullardan biri bir nechta shifrlash algoritmlarini ketma-ket ishlatishdir. Ushbu yondashuv ma'lumotlarni himoya qilish darajasini sezilarli darajada oshirishi mumkin, chunki tajovuzkor bir nechta turli xil algoritmlardan foydalangan holda ma'lumotlarni shifrlashi kerak.

2. Mumkin bo'lgan hujumlarning oldini olish uchun foydalaniladigan shifrlash algoritmlarini vaqti-vaqti bilan yangilab turish zarur [9]. Ko'pgina shifrlash algoritmlarining ishlash muddati cheklangan, chunki vaqt o'tishi bilan zaifliklar aniqlanishi mumkin.

Ushbu maqolada zamonaviy ma'lumotlarni shifrlash algoritmlari tahlil qilingan. AES va RSA kabi eng keng tarqalgan shifrlash algoritmlari ko'rib chiqildi. Ushbu algoritmlarning zaif tomonlari va turli hujum usullari ham muhokama qilindi. Ma'lumotlar xavfsizligi darajasini oshirish uchun keng qamrovli himoya usullaridan foydalanish va ishlatiladigan shifrlash algoritmlarini vaqti-vaqti bilan yangilab turish kerak.

ADABIYOTLAR RO’YHATI

1. Babenko L.K., Ishchukova E.A. Sovremennye algoritmy blochnogo shifrovaniya i metody ikh analiza [Modern block cipher algorithms and methods of their analysis]. M.: Gelios ARV, 2015. 376 p.

2. Mao V. Sovremennaya kriptografiya: teoriya i praktika [Modern Cryptography: Theory and Practice]. M.: Vil'yams, 2005. 768 p.

3. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2009. 372 p.

4. Panasenko S.P. Algoritmy shifrovaniya. Spetsial'nyy spravochnik. [Encryption algorithms. Special Reference Guide.]. SPb.: BKhV-Peterburg, 2009. 576 p.

5. Шаньгин В.Ф. Информационная безопасность и защита информации. - М.: ДМК Пресс, 2014. - 702 с.

6. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования. - М.: ИНФРА-М, 2015. - 869 с.

7. Плёнкин А.П. Симметричное шифрование квантовыми ключами // Инженерный вестник Дона. 2016. №3. URL: ivdon.ru/ru/magazine/archive/n1y2016/3705.

8. Мациборко В.В., Будко А.Ю., Береснев А.Л., Мациборко М.А. Исследование устройств регистрации ионного тока в камере сгорания // Инженерный вестник Дона, 2014, №4. URL: ivdon.ru/ru/magazine/archive/n4y2014/2611/.

9. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации. - 2-е изд. - М.: Юрайт, 2016. - 474 с.